Claims

1. A method for linking between nodes in a distributed computing system, the method comprising:

implementing a domain comprising a first network node and a second network node;

implementing a data object that indicates whether the domain permits links between nodes without verification of user credentials; and

sending a link request from the first network node to the second network node;

establishing a link between the first network node and the second network node without requiring the user credentials if the data object indicates verification of the user credentials is not required.

2. The method of claim 1 in which a connected user makes the link request, and the link is established as a connected user.

3. The method of claim 1 in which a connected user makes the link request as a current user, and the link is established as a current user.

4. The method of claim 3 in which the link request is embedded in a stored object.

5. The method of claim 4 in which the stored object is selected from the list consisting of: a procedure, a function, a view, a trigger.

6. The method of claim 1 in which the second network node comprises a list of untrusted nodes, wherein the link between the first network node and the second network node is not established if the list of untrusted nodes indicates that the first network node is untrusted.

7. The method of claim 1 in which the data object that indicates whether the domain permits links between nodes without verification of user credentials is a flag in a domain object corresponding to the domain.

8. The method of claim 1 further comprising a second domain having a third network node, in which a second link request is sent from the first network node to the third network node, wherein an act of establishing a network link between the first network node and the third network is made only upon verification of user credentials.

9. The method of claim 1 further comprising a second domain having a third network node, in which a second link request is sent from the first network node to the third network node, wherein an act of establishing a network link between the first network node and the third network is made without verification of user credentials.

10. The method of claim 1 in which mutual authentication occurs between the first network node and the second network node.

11. The method of claim 1 in which the first network node passes information to the second network node regarding a prior chain of links related to the link request.

12. The method of claim 11 in which the information regarding the prior chain of links comprises identification of all previous users in the prior chain of links.

13. The method of claim 11 in which the information regarding the prior chain of links comprises identification of previous nodes in prior related links

14. The method of claim 11 in which a last entry in the information is checked for an untrusted user/node combination.

15. The method of claim 14 in which trusted user/node combinations are maintained at a central authority.

16. The method of claim 15 in which the central authority is the directory.

17. The method of claim 14 in which untrusted combinations are stored in a database.

18. The method of claim 1 further comprising:

establishing the link between the first network node and the second network node only upon verification of the user credentials if the data object indicates that user credentials are required.

19. A computer program product that includes a medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process for linking between nodes in a distributed computing system, the process comprising:

implementing a domain comprising a first network node and a second network node;

implementing a data object that indicates whether the domain permits links between nodes without verification of user credentials;

sending a link request from the first network node to the second network node;

establishing a link between the first network node and the second network node without requiring the user credentials if the data object indicates verification of the user credentials is not required.

20. The computer program product of claim 19 in which a connected user makes the link request, and the link is established as a connected user.

21. The computer program product of claim 19 in which a connected user makes the link request as a current user, and the link is established as a current user.

22. The computer program product of claim 21 in which the link request is embedded in a stored object.

23. The computer program product of claim 22 in which the stored object is selected from the list consisting of: a procedure, a function, a view, a trigger.

24. The computer program product of claim 19 in which the second network node comprises a list of untrusted nodes, wherein the link between the first network node and the second network node is not established if the list of untrusted nodes indicates that the first network node is untrusted.

25. The computer program product of claim 19 in which the data object that indicates whether the domain permits links between nodes without verification of user credentials is a flag in a domain object corresponding to the domain.

26. The computer program product of claim 19 further comprising a second domain having a third network node, in which a second link request is sent from the first network node to the third network node, wherein an act of establishing a network link between the first network node and the third network is made only upon verification of user credentials.

27. The computer program product of claim 19 further comprising a second domain having a third network node, in which a second link request is sent from the first network node to the third network node, wherein an act of establishing a network link between the first network node and the third network is made without verification of user credentials.

28. The computer program product of claim 19 in which mutual authentication occurs between the first network node and the second network node.

29. The computer program product of claim 19 in which the first network node passes information to the second network node regarding a prior chain of links related to the link request.

30. The computer program product of claim 29 in which the information regarding the prior chain of links comprises identification of all previous users in the prior chain of links.

31. The computer program product of claim 29 in which the information regarding the prior chain of links comprises identification of previous nodes in prior related links

32. The computer program product of claim 29 in which a last entry in the information is checked for an untrusted user/node combination.

33. The computer program product of claim 32 in which trusted user/node combinations are maintained at a central authority.

34. The computer program product of claim 33 in which the central authority is the directory.

35. The computer program product of claim 33 in which untrusted combinations are stored in a database.

36. The computer program product of claim 19 further comprising:

establishing the link between the first network node and the second network node only upon verification of the user credentials if the data object indicates that user credentials are required.

37. A system of networked nodes in a distributed system, comprising:

a domain;

a first network node associated with the domain;

a second network node associated with the domain; and

a data object associated with the domain, the data object indicating whether a link can be established between the first network node and the second network node without verification of user credentials.

38. The system of claim 37 in which the link is requested by a connected user, and the link is established as a connected user.

39. The system of claim 37 in which the link is requested by a connected user, and the link is established as a current user.

40. The system of claim 37 further comprising a link request embedded in a stored object.

41. The system of claim 40 in which the stored object is selected from the list consisting of: a procedure, a function, a view, a trigger.

42. The system of claim 37 in which the second network node comprises a list of untrusted nodes, wherein the link between the first network node and the second network node is established only upon verification of the user credentials if the list of untrusted nodes indicates that the first network node is untrusted.

43. The system of claim 37 in which the data object that indicates whether the domain permits links between nodes without verification of user credentials is a flag in a domain object corresponding to the domain.

44. The system of claim 37 in which mutual authentication occurs between the first network node and the second network node.

45. The system of claim 37 in which the first network node passes information to the second network node regarding a prior chain of links related to the link request.

46. The system of claim 45 in which the information regarding the prior chain of links comprises identification of all previous users in the prior chain of links.

47. The system of claim 45 in which the information regarding the prior chain of links comprises identification of previous nodes in prior related links

48. The system of claim 45 in which a last entry in the information is checked for an untrusted user/node combination.

49. The system of claim 48 in which trusted user/node combinations are maintained at a central authority.

50. The system of claim 49 in which the central authority is the directory.

ABSTRACT

A method and system for managing access information for users and other entities in a distributed computing system is disclosed. An aspect of the invention relates to current user links between a first computing node and a second computing node. Objects are created/maintained to identify allowable links between computing nodes. Objects can also be created/maintained to store identification of chains of links. The current user link allows access for a user from the first computing node to the second computing node without user authentication by the second computing node. This can be implemented using trust relationships between the first and second computing nodes. Transitive aspects of the trust relationships can be handled by accessing information about chains of users/nodes. In addition, trust relationships can be administered by a local computing node.